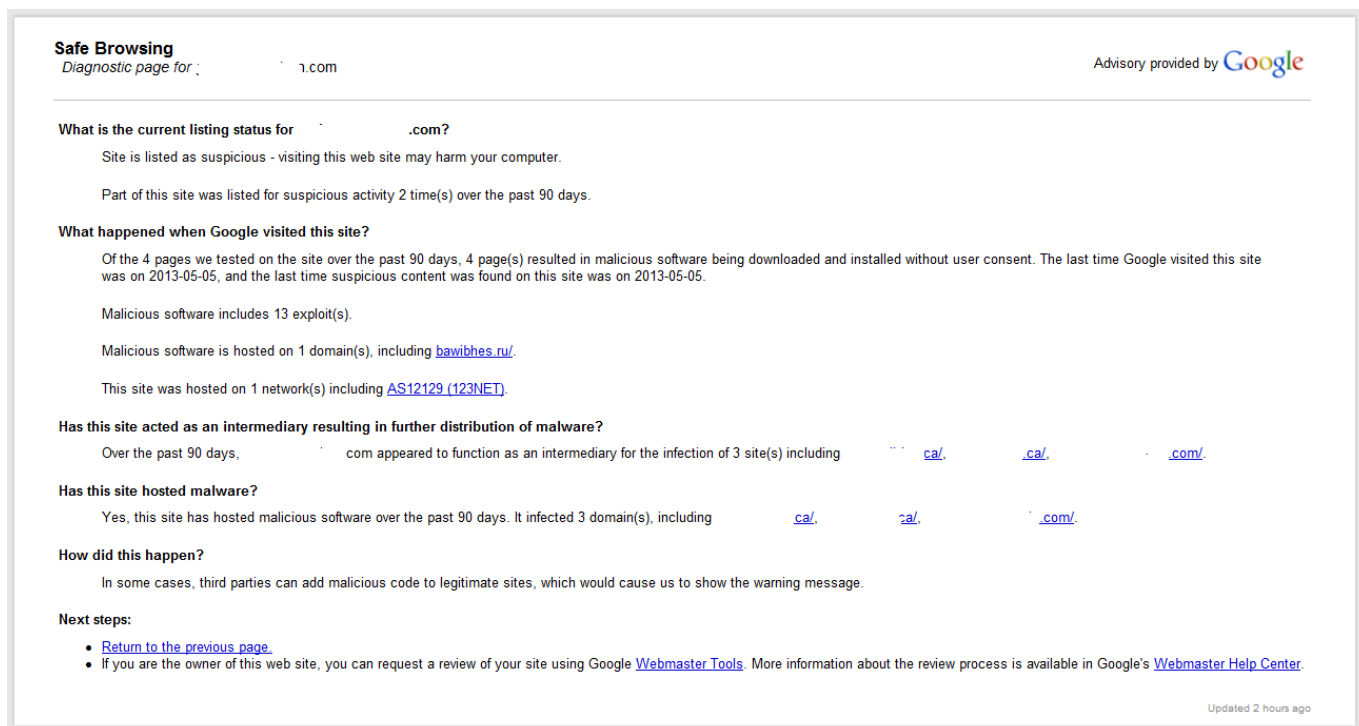


A Drive-By....Website?

By Don Devenney, CD GCWN CIPP/C

I heard a commercial on my office radio last week that interested me so I thought I'd check out the website mentioned in the ad. I opened my web browser, entered the URL and – to my surprise – the next page I saw looked very much like the following (note: domain names have been removed to protect the innocent):



The screenshot shows a "Safe Browsing" diagnostic page from Google. The page title is "Safe Browsing" and it is a "Diagnostic page for" a website with a redacted domain name. The page is provided by Google. The content is as follows:

What is the current listing status for [redacted].com?
Site is listed as suspicious - visiting this web site may harm your computer.
Part of this site was listed for suspicious activity 2 time(s) over the past 90 days.

What happened when Google visited this site?
Of the 4 pages we tested on the site over the past 90 days, 4 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2013-05-05, and the last time suspicious content was found on this site was on 2013-05-05.
Malicious software includes 13 exploit(s).
Malicious software is hosted on 1 domain(s), including [bawibhes.ru/](#).
This site was hosted on 1 network(s) including [AS12129 \(123NET\)](#).

Has this site acted as an intermediary resulting in further distribution of malware?
Over the past 90 days, [redacted].com appeared to function as an intermediary for the infection of 3 site(s) including [\[redacted\].ca/](#), [\[redacted\].ca/](#), and [\[redacted\].com/](#).

Has this site hosted malware?
Yes, this site has hosted malicious software over the past 90 days. It infected 3 domain(s), including [\[redacted\].ca/](#), [\[redacted\].ca/](#), and [\[redacted\].com/](#).

How did this happen?
In some cases, third parties can add malicious code to legitimate sites, which would cause us to show the warning message.

Next steps:

- [Return to the previous page.](#)
- If you are the owner of this web site, you can request a review of your site using Google [Webmaster Tools](#). More information about the review process is available in Google's [Webmaster Help Center](#).

Updated 2 hours ago

So what happened? Well, the last time Google scanned the website in question they were able to determine that the site was being used to distribute malicious code or “malware” so they put this warning up. Using “innocent” websites to distribute malware has become an increasingly popular way for cyber criminals to infect computers and it’s known as a “drive-by attack” or “drive-by download”. Here’s how they do it:

The cyber-criminal group will break into a website and edit the code of the page so that it delivers malware to the site visitor. Usually this works by the bad guys creating their own webpage or part of a webpage and then loading it into a section of the website – usually as a button, a banner ad or some other area you’re likely to click on – in such a way that you won’t notice it. It’s a very effective method of attacking user’s machines as it’s normally concealed so that the user doesn’t see it.

The attack is called a “drive-by” attack because you are unlikely to have noticed it happened...you just “cruise on by” the site, click a link and you’re infected. The criminals take advantage of known vulnerabilities in operating systems or popular software, and try to get you

to click on a link or download a file that they have crafted to look like something you'd expect to see on the site you're visiting. At this point it's pretty easy for unsuspecting site visitors to unwittingly download and run the malicious software that will infect their computers. They'll click on a link, an image, a button, etc. and that will download and run the bad software. The software the criminals are distributing runs the gamut from fake "your computer is infected" warnings that try to get you to buy their "virus removal software" to key loggers that record every keystroke you make (including the usernames and passwords to your on-line accounts) and send the results to one of the criminal's servers. Oh, and this kind of attack can be tailored to the operating system of the computer you're using so whether you're using Windows or Mac you can still be vulnerable.

So how can you protect yourself against a drive-by attack? Here are a few steps you can take:

- Keep all software updated with the latest service packs and security updates. This is the most effective practice in preventing systems from exploitation. ALL software – operating systems, Web browsers, productivity suites (i.e. Word, Excel, etc.) and other programs like Adobe Reader, iTunes, Java, Flash, etc. need to be kept up-to-date.
- Make sure that the account you use for your day-to-day activities does NOT have administrative privileges. Create a separate administrator account that you use when required. Since "standard" user accounts can't install software, using a standard user account may prevent the malicious software from loading.
- Newer software is better. The data suggests attackers are more successful when targeting older operating systems, Web browsers and other software.
- Use anti-malware software from a trusted vendor and keep it up-to-date.
- Be careful who you talk to on-line, be selective about the emails you open and especially cautious about the attachments and links you click on.
- Leverage the protection technologies that are available in modern Web browsers and search engines. I've mentioned Google already; the SmartScreen filter built into Internet Explorer is an example of another tool that helps protect against sites known to be distributing malware by blocking navigation to malicious sites or downloads.
- Know how your anti-virus / malware software behaves when it blocks a virus or malware. That way you're less likely to be fooled by malicious software that pretends to find "viruses" on your computer.

I once heard the Internet described as being like "a bad neighbourhood at 2am" and there's probably a fair bit of truth in that statement. However if you add some "armour" to your computer in the form of software updates and anti-malware software and are careful where and how you "drive" you should be able to navigate the Internet in relative safety.

Don Devenney is a member of the Server, Networks and Telecom Infrastructures team at Royal Roads University and is a GIAC Certified Windows Security Administrator.